

## AFFIDAVIT

I, Patrick Hanna, being duly sworn, depose and state as follows:

### Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and currently assigned to the Burlington Resident Agency in Vermont. I have been an FBI Special Agent for 20 years. My duties as an FBI Special Agent include investigating violations of Title 18 of the United States Code as they pertain to corporate fraud, complex financial crimes, embezzlement, public corruption, money laundering and related white-collar crimes, as well as violent crimes and criminal enterprises. I have participated in investigations of criminal violations of various federal laws. I have executed search and arrest warrants, interviewed and interrogated subjects, witnesses, and victims, and conducted surveillance. In the course of these investigations, I have gained an understanding of current technology, to include computers and online accounts, cellular telephones and associated records and data, and have conducted analyses of the data related to such accounts and devices, for the purpose of solving and proving crimes.

2. I make this affidavit in support of an application for a search warrant directing Microsoft Corporation to produce data associated with beratay@live.com (Subject Account) as described in Attachment A, that would allow the extraction and examination of data from a computer tower that this Court has already authorized me to search, as well as data stored on Microsoft servers in order to search and seize data described in Attachment B. As described below, forensic examiners have attempted to extract data from the tower but found that the data is encrypted. This application seeks a warrant to order Microsoft to produce data that would allow forensic examiners to unlock the data on the tower so that this Court's prior order can be executed. I have also determined that Microsoft appears to hold cloud-based data that may contain evidence of the crimes described below.

3. On May 19, 2022, the federal grand jury sitting in Burlington, Vermont, charged Serhat Gumrukcu with conspiring with Berk Eratay and others between May 2017 and February 2018 to pay someone to murder Gregory Davis, whose body was discovered on January 7, 2018. On December 13, 2022, the grand jury returned an additional charge against Gumrukcu and Eratay, alleging that the two conspired between 2015 and 2018 to commit wire fraud by misrepresenting various relevant facts to Davis and Gregory Gac. As discussed below, there is probable cause to believe that Gumrukcu was involved in this murder-for-hire conspiracy, along with Eratay, Aron Ethridge, and Jerry Banks. Davis's murder involved the following federal crimes: kidnapping, in violation of 18 U.S.C. § 1201; murder to obstruct justice, in violation of 18 U.S.C. § 1512(a)(1); murder for hire, in violation of 18 U.S.C. § 1958; and wire fraud, in violation of 18 U.S.C. § 1343.

4. This case is being investigated by the FBI and the Vermont State Police (VSP). Since this affidavit is being submitted for the limited purpose of establishing probable cause to search data already in law enforcement's custody, I have not included details of every aspect of the investigation. Except as otherwise noted, the information contained in this affidavit is based

upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and my review of documents and records.

Probable Cause

5. On September 13, 2022, I obtained a search warrant for a several devices used by Berk Eratay prior to his arrest, including a black CLX PC computer tower (Subject Device). Exhibit 1. I have successfully obtained search warrants for each of Eratay's devices that I have been able to locate. I believe that any location or device holding data generated by Eratay is relevant to my investigation. I have attached the affidavit in support of the application for Subject Device warrant and adopt that as probable cause here. Exhibit 2. That affidavit and its attachments accurately reflect evidence developed at that time. Since then, I have learned additional facts. One aspect of the investigation that should be updated is my understanding about the use of two Google email accounts (muratgumrukcu@gmail.com and murtagumrukcu@gmail.com) that appeared to be used by Murat Gumrukcu, Serhat Gumrukcu's brother. I have developed substantial evidence that Berk Eratay and/or Serhat Gumrukcu generated the emails supposedly from Murat Gumrukcu, who I have learned could not speak English fluently. This evidence, along with other evidence, supported the additional wire fraud conspiracy charge against Serhat Gumrukcu and Berk Eratay in the Second Superseding Indictment. Thus, at this time, Murat Gumrukcu may have not been involved in the murder plot. With this additional information, I incorporate the other information in Exhibit 2 and its attachments for purposes of this affidavit.

6. The Subject Device was sent to FBI's Evidence Control unit and CART (Computer Analysis Response Team) unit in the Albany Field Office where the Seagate hard drive was removed from the device in order for the CART unit to generate a forensic image for review, but CART was initially unsuccessful. CART personnel then requested assistance from the Digital Forensic Analysis Unit (DFAU) to recover data from the Seagate hard drive. DFAU successfully generated a forensic image of the hard drive.

7. On or about November 2, 2022, the forensic image of the hard drive was made available for analysis. However, CART personnel were not able to analyze the forensic image of the hard drive because data on the drive was encrypted with BitLocker, a Microsoft encryption product. Due to the drive containing a BitLocker encryption lock that requires a unique key, investigators are unable to review the contents of the Subject Device. The CART forensic software would allow the encrypted data to be unencrypted with the BitLocker recovery key if available to the examiners.

8. Based on my experience and conversations with forensic examiners, I know that Microsoft provides support for users of Microsoft hardware, software and/or products running or operating with Microsoft products in the event the user somehow does not know or loses the BitLocker key. Specifically, Microsoft maintains on their servers and/or in their records a BitLocker recovery key for devices locked by BitLocker if the user chooses. If the user so chooses, the BitLocker recovery keys are stored in the user's Microsoft account.

9. I have learned the following, among other things, about Microsoft:

a. Microsoft is a United States company that produces the Microsoft Windows operating system (OS). The Windows OS offers computer users the option to encrypt their device using so-called BitLocker encryption.

b. Microsoft provides a variety of services that can be accessed from Microsoft devices or, in some cases, other devices via web browsers or mobile and desktop applications apps. One such service is OneDrive:

i. OneDrive is a file hosting, storage, and sharing service provided by Microsoft. OneDrive can be used through numerous OneDrive-connected services and can also be used to store Windows OS device backups and data associated with third-party apps.

ii. OneDrive services allow users to create, store, access, share, and synchronize data on various devices that use Windows OS. A OneDrive user can save data to Microsoft cloud servers, including selected data or even full computer back-ups of data on a particular device. Users can set up their accounts so that data is automatically saved to these cloud-based servers.

iii. BitLocker Device Encryption encrypts Windows devices for data security purposes, and it can store a 48-character recovery key in the user's online Microsoft account.

c. Microsoft services are accessed with a "Microsoft Account," an account created during the setup of a Microsoft device. A single Microsoft Account can be linked to multiple Microsoft services and devices, serving as a central authentication and syncing mechanism.

d. A Microsoft Account takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit a Microsoft-provided email address (often ending in @outlook.com, @hotmail.com, or @live.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Microsoft Account can be used to access most Microsoft services only after the user accesses and responds to a "verification email" sent by Microsoft to that "primary" email address. Additional email addresses (alternate, rescue, and "notification" email addresses) can also be associated with a Microsoft Account by the user.

e. Microsoft captures information associated with the creation and use of a Microsoft Account. During the creation of a Microsoft Account, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Microsoft. The subscriber information and password associated with a Microsoft Account can be changed by the user through the Microsoft Account on Microsoft's website. In addition, Microsoft captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address



("IP address") used to register and access the account, and other log files that reflect usage of the account.

f. Additional information is captured by Microsoft in connection with the use of a Microsoft Account to access certain services. For example, Microsoft maintains connection logs with IP addresses that reflect a user's sign-on activity for Microsoft services such as Windows, OneDrive, Outlook, and the Microsoft Account on Microsoft's website. Connection logs and requests to remotely lock or erase a device are also maintained by Microsoft.

g. Microsoft also maintains information about the devices associated with a Microsoft Account. When a user activates or upgrades a Windows OS device, Microsoft captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Microsoft also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. Microsoft also retains records related to communications between users and Microsoft customer service, including communications regarding a particular Microsoft device or service, and the repair history for a device.

h. In addition to backing up a BitLocker recovery key to a Microsoft Account, a user may also store a copy of a BitLocker recovery key to a local file.

10. In 2020, I obtained information from Microsoft showing that in 2013 Eratay opened a Microsoft account associated with beratay@live.com. The Microsoft account records listed the services used at that time as Office 365, Xbox Live, and Groove Music.

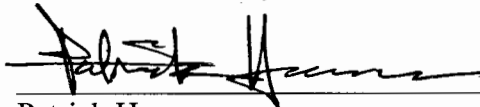
11. In 2022, I obtained a search warrant for data on an Apple iPhone possessed by Eratay prior to his arrest. I have reviewed data extracted from that phone and found multiple pieces of data that were seized as relevant to the matters under investigation. I also found emails from "OneDrive photos@onedrive.com" to beratay@live.com with the Subject "Your memories from this day" which indicate that Eratay was using the OneDrive cloud service. In addition, data from March 18, 2022, shows a Google Chrome web history link to the URL <https://onedrive.live.com/> and a Visit Source as "Synced," which I believe indicates that some Eratay device was syncing to the OneDrive cloud service. On the same date, the data also reflects a Google Chrome web visit to the same URL and listing the Artifact type as "Cloud Services URLs." Based on this data, I believe that Eratay continued to use his beratay@live.com Microsoft account up to the time of his arrest, that Eratay stored relevant information on Microsoft servers, and that his Microsoft account will contain evidence of the crimes listed above.

12. The forensic imaging process of the Subject Device resulted in the imaging software creating a log file. The examiners reviewed the log file and noted that the log confirmed certain data on the hard drive was encrypted by BitLocker. The log also identified a recovery key ID, which identifies the hard drive that is encrypted.

13. The recovery key ID for the Subject Device is 7D596524-F4A5-46DC-BC86-AD30C89CA39D. As noted above, to review the forensic image, it is necessary to obtain the recovery key for the hard drive with BitLocker recovery password ID: 7D596524-F4A5-46DC-BC86-AD30C89CA39D. Based on my research and conversations with forensic examiners, Microsoft would use this recovery key ID as a reference to find the recovery key. Moreover, the discovery of this recovery key ID indicates that the Subject Device's BitLocker recovery key may be maintained by Microsoft in the user's Microsoft Account.

14. I believe that there is probable cause to believe that the data sought in Attachment A associated with the Subject Account contains evidence of the crimes listed above as described in Attachment B, including a BitLocker recovery key for the Subject Device, allowing forensic analysts to access the otherwise encrypted Subject Device to execute an earlier search warrant of the Subject Device.

Dated at Burlington, in the District of Vermont, this 24<sup>th</sup> day of March 2023.



Patrick Hanna  
Special Agent - FBI

Sworn to and subscribed before me this 24 day of March 2023.



Honorable Geoffrey W. Crawford  
United States District Judge